ON A THEOREM OF FRIEDLANDER AND IWANIEC

JEAN BOURGAIN AND ALEX KONTOROVICH

Abstract. In [FI09], Friedlander and Iwaniec studied the so-called Hyperbolic Prime Number Theorem, which asks for an infinitude of elements $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ such that the norm squared

$$\|\gamma\|^2 = a^2 + b^2 + c^2 + d^2 = p,$$

a prime. Under the Elliott-Halberstam conjecture, they proved the existence of such, as well as a formula for their count, off by a constant from the conjectured asymptotic. In this note, we study the analogous question replacing the integers with the Gaussian integers. We prove unconditionally that for every odd $n \geq 3$, there is a $\gamma \in \mathrm{SL}(2,\mathbb{Z}[i])$ such that $\|\gamma\|^2 = n$. In particular, every prime is represented. The proof is an application of Siegel's mass formula.

1. Introduction

The Affine Linear Sieve, introduced by Bourgain, Gamburd and Sarnak [BGS06], aims to produce prime points for functions on orbits of groups of morphisms of affine space. Friedlander and Iwaniec [FI09] considered the case of the full modular group $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, with the function being the norm-square. Let S be the set of norm-squares in Γ, that is,

$$S := \left\{ n \in \mathbb{Z}_+ \ : \ n = \|\gamma\|^2 \text{ for some } \gamma \in \mathrm{SL}(2,\mathbb{Z}) \right\}.$$

They proved, assuming an approximation to the Elliott-Halberstam conjecture, that S contains infinitely many primes.[1]

Unconditionally, one can easily show the existence of 2-almost primes in S. Indeed, for any $x \in \mathbb{Z}$, the parabolic elements

$$n_x := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Date: August 5, 2010.

Bourgain is partially supported by NSF grant DMS-0808042.

Kontorovich is partially supported by NSF grants DMS-0802998 and DMS-0635607, and the Ellentuck Fund at IAS.

[1]Moreover they gave a formula for the count of norm-squares (with multiplicities), off by a constant from the conjectured asymptotic.

are in Γ, and their norm-square is $\|n_x\|^2 = x^2 + 2$. Then Iwaniec's theorem [Iwa78] produces infinitely many 2-almost primes in S.

In this note, we ask an analogous question, replacing the integers in $\mathrm{SL}(2,\mathbb{Z})$ by the Gaussian integers, $\Gamma = \mathrm{SL}(2,\mathbb{Z}[i])$. We prove unconditionally the following

Theorem 1.1. *The set*

$$S := \left\{ n \in \mathbb{Z}_+ \ : \ n = \|\gamma\|^2 \text{ for some } \gamma \in \mathrm{SL}(2,\mathbb{Z}[i]) \right\}$$

contains all odd integers $n \geq 3$. In particular, it contains all primes.

The proof, given in the next section, is an application of Siegel's mass formula [Sie35]. The argument is sufficiently delicate that it cannot replace the Gaussian integers above by the ring of integers of another number field, even an imaginary quadratic extension (as suggested to us by John Friedlander), see Remark 2.6.

We thank Zeev Rudnick and Peter Sarnak for conversations regarding this work.

2. Sketch of the Proof

For odd $n \geq 3$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a = a_1 + ia_2$, etc., the conditions $n = \|\gamma\|^2$ and $\gamma \in \mathrm{SL}(2,\mathbb{Z}[i])$ imply

$$\begin{cases} \|\gamma\|^2 = a_1^2 + b_1^2 + c_1^2 + d_1^2 + a_2^2 + b_2^2 + c_2^2 + d_2^2 = n, \\ \mathfrak{Re}(\det\gamma) = a_1 d_1 - b_1 c_1 + b_2 c_2 - a_2 d_2 = 1 \\ \mathfrak{Im}(\det\gamma) = a_1 d_2 + a_2 d_1 - b_1 c_2 - b_2 c_1 = 0. \end{cases} \tag{2.1}$$

Changing variables

$$\begin{aligned} a_1 &\to (y_1 + y_4)/2, & b_1 &\to (y_3 + y_2)/2, \\ c_1 &\to (y_3 - y_2)/2, & d_1 &\to (y_1 - y_4)/2, \\ a_2 &\to (y_5 + y_8)/2, & b_2 &\to (y_7 + y_6)/2, \\ c_2 &\to (y_7 - y_6)/2, & d_2 &\to (y_5 - y_8)/2, \end{aligned}$$

the system (2.1) becomes

$$\begin{cases} y_3^2 + y_4^2 + y_5^2 + y_6^2 = n - 2, \\ y_1^2 + y_2^2 + y_7^2 + y_8^2 = n + 2, \\ y_1 y_5 + y_2 y_6 - y_3 y_7 - y_4 y_8 = 0. \end{cases} \tag{2.2}$$

Write

$$F = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad G_n = \begin{pmatrix} n+2 & & \\ & & n-2 \end{pmatrix},$$

and

$$X = \begin{pmatrix} y_1 & y_2 & -y_7 & -y_8 \\ y_5 & y_6 & y_3 & y_4 \end{pmatrix},$$

so that (2.2) becomes

$$XF\,{}^tX = G_n. \tag{2.3}$$

Recall Siegel's [Sie35] mass formula, cf. [Cas78, Appendix B, equations (3.10) to (3.17)]. Clearly F is positive definite and alone in its genus, and hence the number $\mathcal{N}(F, G_n)$ of solutions X to (2.3) is given by

$$\mathcal{N}(F, G_n) = \prod_{p \le \infty} \alpha_p(F, G_n), \tag{2.4}$$

where the local densities α_p are given as follows. For $p < \infty$, they are defined by

$$\alpha_p(F, G_n) = p^{-5t} \cdot \#\big\{X (\mathrm{mod}\, p^t) : XF\,{}^tX \equiv G_n (p^t)\big\}, \tag{2.5}$$

for t sufficiently large. For $p = \infty$, we have

$$\alpha_\infty(F, G_n) = 2\pi^3 (n^2-4)^{1/2}.$$

Remark 2.6. In complete generality, it is notoriously difficult to compute the local densities α_p and extract information such as non-vanishing, see e.g. the formulae in [Yan98, Yan04]. The main problem being how large is "sufficiently large" for t in (2.5) with a given p. In our special case of $\Gamma = \mathrm{SL}(2, \mathbb{Z}[i])$, the literature is sufficient to carry out the task.

For $p \neq 2$, both the ramified and unramified local densities can be evaluated as in e.g. [Kit83, Theorem 2]. We turn first to the case p is unramified, $p \nmid (n^2-4)$. Then

$$\alpha_p(F, G_n) = \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{\chi_p(4-n^2)}{p}\right),$$

where $\chi_p = \left(\frac{\cdot}{p}\right)$ is the quadratic character mod p. For ramified primes $p \geq 3$, write $n+2 = mp^a$ and $n-2 = kp^b$ with $(mk, p) = 1$. Assume $0 \leq a \leq b$ (otherwise reverse their roles). Then if $a + b \equiv 0 (\mathrm{mod}\, 2)$,

$$\alpha_p(F, G_n) = \frac{(p+1)\left((p^{a+1}-1)\left(\chi_p(-mk)-1\right) + (a+1)\,(p^2-1)\,p^{(a+b)/2}\right)}{p^{3+(a+b)/2}}.$$

Otherwise, if $a+b \equiv 1 (\mathrm{mod}\, 2)$, then

$$\alpha_p(F, G_n) = \frac{(p+1)^2\left((a+1)(p-1)p^{(a+b+1)/2} - (p^{a+1}-1)\right)}{p^{3+(a+b+1)/2}}.$$

Inspection shows that these terms never vanish.

It remains to evaluate the dyadic density, α_2. As shown by Siegel, see [Rei56], for n odd (and hence n^2-4 odd), it is sufficient to evaluate (2.5) for $t=3$, that is, compute the number of solutions $\mathrm{mod}\, 2^3 = 8$. One can compute explicitly that for any odd n, the number of solutions to (2.5) $\mathrm{mod}\, 8$ is 49 152. Since $8^5 = 32\,768$, we have

$$\alpha_2(F, G_n) = \frac{3}{2}.$$

In conclusion, the α_p's never vanish so there are no local obstructions for odd n to be represented, and hence the set S of norm-squares in $\mathrm{SL}(2, \mathbb{Z}[i])$ contains all the primes. (The prime 2 is in S since it is the norm squared of the identity matrix.)

References

[BGS06] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Sieving and expanders. *C. R. Math. Acad. Sci. Paris*, 343(3):155–159, 2006.

[Cas78] J. W. S. Cassels. *Rational Quadratic Forms*. Number 13 in London Mathematical Society Monographs. Academic Press, London-New York-San Francisco, 1978.

[FI09] John B. Friedlander and Henryk Iwaniec. Hyperbolic prime number theorem. *Acta Math.*, 202(1):1–19, 2009.

[Iwa78] Henryk Iwaniec. Almost-primes represented by quadratic polynomials. *Invent. Math.*, 47:171–188, 1978.

[Kit83] Yoshiyuki Kitaoka. A note on local densities of quadratic forms. *Nagoya Math. J.*, 92:145–152, 1983.

[Rei56] Irma Reiner. On the two-adic density of representations by quadratic forms. *Pacific J. Math.*, 6:753–762, 1956.

[Sie35] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen. *Ann. of Math. (2)*, 36(3):527–606, 1935.

[Yan98] Tonghai Yang. An explicit formula for local densities of quadratic forms. *J. Number Theory*, 72(2):309–356, 1998.

[Yan04] Tonghai Yang. Local densities of 2-adic quadratic forms. *J. Number Theory*, 108(2):287–345, 2004.

E-mail address: bourgain@ias.edu

IAS, Princeton, NJ

E-mail address: avk@math.ias.edu

IAS and Brown University, Princeton, NJ